(S//SI) Targeting Terrorist Internet Traffic

FROM: [redacted]
Technical Director, Protocol Exploitation Branch, CES/Systems Analysis (S31212)
Run Date: 03/30/2004

FROM: [redacted]
Technical Director, Protocol Exploitation Branch, CES/Systems Analysis (S31212)

(S//SI) On February 14, 2004, a terrorist on the Counterterrorism top ten list walked into a web cafÃ© in Iraq and logged into an MSN Messenger account. Little did this terrorist know that NSA knew his login name and that Counterterrorism analysts were alerted to his traffic. Unfortunately, the analysts were unable to do much with it, as the target never talked to anyone and he had few names on his buddy list.

(S//SI) The analysts wanted to look at all of the traffic generated by the terrorist but were unable to do so... The web cafÃ© used an inexpensive device known as a Network Address Translator (NAT) to share the Internet connection to all the computers in the cafÃ©. There were many people in the cafÃ© and the NAT mixed the computer sessions from all of the users together. Luckily, a fledgling service known as DISTANTFISH had just been deployed to Menwith Hill Station, and this new system was able to find the desired terrorist traffic.

(S//SI) Project DISTANTFISH was created to target terrorist traffic on the Internet by providing two important services. First, it provides a database for discovering account identities for known terrorists to use as strong selectors (i.e. login names, e-mail addresses, or other elements that can be associated with a particular individual). Second, it provides information on which the same user generated computer sessions. Thus, if one session contains a strong selector for a terrorist, then all sessions can be collected. At the heart of this capability is an association service that can track an individual computer by the way it generates packets.

(S//SI) From this association service, the DISTANTFISH team members were able to determine that the terrorist generated 107 computer sessions over eleven minutes, thus separating this traffic from that of the other 16 people in the web cafÃ©. As most of the supporting software is still under development, the data was manually examined resulting in the discovery of two additional MSN Messenger accounts and two Yahoo web mail accounts that the terrorist used, but that NSA had been unaware of. Since terrorists often abandon accounts for new ones, having a complete picture of the accounts used is critical for targeting the terrorists' traffic.

(U) Transforming DNI Selection and Filtering

(S//SI) The need to greatly expand the existing DNI Surgical Survey capability has been recognized by Data Acquisition and Analysis and Production, placing this task on a list of twelve critical hard DNI problems known as the DA Dozen. The proposed solution is referred to as Persona Session Collection (PSC) and, to work, relies on strong selectors and user session association. DISTANTFISH provides critical capability on both and was highlighted as an important component to transforming DNI selection and filtering.

(S//SI) PSC works by processing application layer protocols to extract certain metadata fields that work as strong selectors for the client of the current application. These selectors are usually login names, client e-mail addresses, user numbers, and other unique metadata. If a selector is found to be that of a known terrorist, that session, as well as all others generated by the terrorist, is forwarded to NSA for analysis. The DISTANTFISH association algorithms are the primary way of determining which sessions the terrorist generated when the access is traditional passive collection. The collection of all user sessions is called the Aggregate Session and can be achieved by other methods, especially active efforts.

(S//SI) However, PSC assumes that the strong selectors for a terrorist are known. The second objective for DISTANTFISH is to associate all strong selectors for SIGINT targets and store them

in a database. Intelligence analysts use the database to discover new identities to add to the selectors for that terrorist. Work on this database has begun, but much work remains.

(U) Moving Forward

(S//SI) Menwith Hill Station has over fifty hits a day on known terrorists accounts. This success has accelerated the work on the DISTANTFISH identity database and on integrating the association information into sustained processing systems. In the coming months, traffic related to all hits will be associated and presented to analysts together. The terrorist identity discovery database being developed in the Target Analysis Cell (TAC/TDS) will also come on line. When that day comes, terrorists will find it difficult to blend in to the crowd, allowing NSA and US troops to target terrorists before they can target us.

(U) More Information

(U//FOUO) DISTANTFISH Project Webpage
